E-SAFETY POLICY

ELTHORNE PARK HIGH SCHOOL
Status: non-statutory policy

Reviewed and updated:	Jan 2024
Next review:	Jan 2026

SLT Member Responsible for Policy Review	David White - Deputy Headteacher
Governors with Responsibilities for E-Safety	Matthew Williams – Governor

The following Acts of Parliament have been referenced when considering e-safety at Elthorne Park High school. These are listed below with details at appendix 1.

- Communications Act 2003 (section 127).
- Computer Misuse Act 1990 (sections 1–3).
- Copyright, Designs and Patents Act 1988.
- Counter-terrorism and Security Act 2015 (section 26)
- Criminal Justice Act 2003.
- Criminal Justice and Immigration Act 2008 (section 63).
- Data Protection Act 1998.
- Data Protection Act 2018 (General Data Protection Regulation (GDPR)).
- Education and Inspections Act 2006.
- Malicious Communications Act 1988 (section 1).
- Obscene Publications Act 1959 and 1964.
- Protection from Harassment Act 1997.
- Public Order Act 1986 (sections 17–29).
- Racial and Religious Hatred Act 2006.
- Regulation of Investigatory Powers Act 2000.
- Sexual Offences Act 2003.

The school has also drawn on the following guidance when reviewing its policy and procedures:

The DFE non-statutory guidance ‘Teaching online safety in school’ June 2019 has also been considered. The DFE's statutory guidance on ‘Keeping children safe in education’ (September 2023) annex on online safety has also been considered.

This policy should also be read in conjunction with the following CEFM policies:

- CEFM’s portfolio of ICT policies available at https://cefmi.cefm.co.uk/Module/278.
- Anti-bullying.
- Safeguarding & Child protection.
- Behaviour policy
- Internal data security.
- Social media policy

CEFM’s education updates May 2020ii ‘Online safety education’, January 2016ii ‘Online safety’ and July 2016i ‘Keeping children safe in education’ have also been considered.

CEFM’s questions and answers ‘Protection against hacking’ June 2017 and ‘Pupils exchanging digital images’ February 2015 and ‘Phone hacking’ March 2013 has also been considered.

The General Data Protection Regulation (GDPR) came into effect in May 2018 and must be heeded by schools whenever personal data is processed. Ofsted inspections will be looking at schools’ compliance.

Ofsted’s briefing for section 5 Inspection ‘Inspecting e-safety in schools’ (September 2018) is designed to provide detailed support for inspectors when reviewing a school’s e-safety provision. It also states that for a school to be considered ‘outstanding’ pupils will have ‘an excellent understanding of how to stay safe online and of the dangers of inappropriate use of mobile technology and social networking sites’.

Ofsted’s ‘Inspecting safeguarding in early years, education and skills settings’ September 2019 also has also been considered in terms of online safety.

UK Council for child internet safety (UKCCIS) has a helpful guide to advise governors on good practice in child internet safety ‘Online safety in schools and colleges: Questions from the governing board’ – www.gov.uk/government/publications/online-safety-in-schools-and-colleges-questions-from-the-governing-board.

UKCCIS Education Working Group also has an interesting report: Online safety in education report (December 2015) explaining what schools should be doing about online safety of their pupils.

Since 2019 UKCCIS is now known as UKCIS because it has taken on the role of improving internet safety for all ages.

Background

The school makes both staff and pupils aware of the dangers of using electronic communication as well as its undoubted benefits. The DFE non-statutory guidance ‘Teaching online safety in schools’ June 2019 document for assisting teachers in the delivery of online safety education has been utilised and considered when reviewing this policy.

The DFE's statutory guidance ‘Keeping children safe in education’ (September 2023) outlines the responsibilities that schools and colleges have in safeguarding children including reference to e-safety. The document requires schools to ensure that:

- Pupils are taught about safeguarding, especially against online abuse such as bullying and sexual abuse by exploitation online.
- They have appropriate filtering and monitoring systems in place on the school’s ICT systems so that no pupil can access harmful content.
- They are careful that ‘over blocking’ does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.
- They develop methods whereby staff are alert to changes in children’s behaviour which could indicate that they may be, in need of help or protection from radicalisation via the internet or social media. Staff should use their judgement and act proportionately, which may include making a referral to the Channel programme under the school’s prevent duty.
- They include online safeguarding in all safeguarding training for staff.

The Ofsted briefing for section 5 Inspection *‘*Inspecting e-safety in schools’ (September 2018) has been used designed to provide detailed support for inspectors when reviewing a school’s e-safety provision. The briefing defines e-safety in the ‘context of an inspection’ as a school’s ability:

- To protect and educate pupils and staff in their use of technology.
- To have the appropriate mechanisms to intervene and support any incident where appropriate.

The briefing paper states that the breadth of issues classified within e-safety is considerable, but can be categorised into three areas of risk:

- Content – being exposed to illegal, inappropriate or harmful material.
- Contact – being subjected to harmful online interaction with other users.
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm.

With regard to online safeguarding of pupils Ofsted’s ‘Inspecting safeguarding in early years, education and skills settings’ September 2018 emphasises that inspectors will:

- Look for evidence that appropriate filters and monitoring systems are in place to protect pupils from potentially harmful online material.
- Discuss online safety in their discussions with pupils (covering topics such as online bullying and safe use of the internet and social media).
- Will investigate what the school does to educate pupils in online safety and how the school deals with issues when they arise.

Personal data held or processed by the school
Under the General Data Protection Regulation schools are responsible for higher standards of e-safety and security of all personal data that they process. Ofsted inspectors will consider schools’ compliance with these regulations when conducting school inspections.

E-SAFETY POLICY

Introduction

Today's pupils are growing up in a world where online and offline life is almost seamless. This offers many opportunities but also creates challenges, risks and threats. At Elthorne Park High school, we try to equip our pupils with the knowledge to be able to use technology to their best advantage in a safe, considered and respectful way.

Our school community recognises the importance of treating e-safety as an ever-present serious safeguarding issue and its teaching as a whole school issue and the responsibility of all staff. It is important to protect and educate both pupils and staff and have supportive mechanisms, policies and protocols in place to protect and support the school community.

Ofsted reviews e-safety measures in schools and there are numerous Acts of Parliament which relate when considering the safeguarding of both staff and pupils in schools. The safeguarding aspects of e-safety are evident in all our ICT/safeguarding policies and procedures throughout the school and it is essential that this constantly developing area of technology is kept under review.

It is also critical to ensure the safety and security of all personal data that the school holds and processes. Under the General Data Protection Regulation, the school is responsible for exacting standards of safety and security of personal data that may be processed.

This policy links all the ICT, safeguarding, social media and other policies and procedures to reflect how the school deals with e-safety issues on a daily basis. The documents referred to in this e-safety policy have been developed by various including consultation with the e-Safety group:

- Governors, including the link governor for e-safety – Matthew Williams (parent governor)
- Headteacher– Eliot Wong
- Deputy Headteacher, Safeguarding Lead, E-safety co-ordinator - David White
- ICT technical support staff. Arpit Bhargava
- Head of PSHCE – Alicia Crix
- IT Network Manager – Arpit Bhargava
- Data Manager & GDPR lead – Shane Ryan (for 23-25 I Serrao has taken over as GDPR lead)
- Teachers and support staff. Kester Lange – Subject Leader Computing.
- Pupils. Invited to e-Safety policy review meetings.
- Parents/carers – parent governor.

Objectives and targets

This policy is aimed at making the use of electronic communication at Elthorne Park High School school as safe as possible. This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to, and are users of, school ICT systems, both in and out of school.

Action plan

The school will deal with any e-safety incidents which arise by invoking this policy, other ICT policies and the associated behaviour and anti-bullying policies. The school will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school and take appropriate action.

Any breaches of safety of personal data held by the school that may arise will be dealt with as soon as they come to light and the appropriate authorities notified.

The following sections outline:

- The roles and responsibilities for e-safety of individuals and groups within the school, and how they will receive education/training to fulfil those roles.
- How the infrastructure is managed.
- How e-safety is considered in the curriculum.
- The protocols on using digital images.
- The protocols on data protection.
- The protocols for handling electronic communication.
- Awareness of and dealing with inappropriate use of electronic media.

Roles and responsibilities – governors

- Filtering and monitoring is an important part of the online safety picture at Elthorne Park High school and the governors ensure that appropriate filters and monitoring systems are in place on the school's ICT resources.

  The school uses the following filtering and monitoring systems:
- Smoothwall – filtering system
- Impero – monitoring system
- LGfL – filtering system

- Governors will ensure compliance with the Data Protection Act and the GDPR for all personal data held.
- Governors will ensure that pupils are taught about e-safety, for example through personal, social, health and economic education (PSHE) and relationships and sex education (RSE) and Computing curriculum at Elthorne Park High school.
- Governors are responsible for the approval of the e-safety policy, for reviewing the effectiveness of the policy and for dealing with issues when they arise.
- A nominated link governor for e-safety is appointed as a member of the school's e-safety committee.
- Governors are responsible for ensuring we have a clear policy on safe access to the internet.
- Governors receive e-safety training/awareness sessions as part of their cycle of meetings and safeguarding training.

Roles and responsibilities – headteacher and senior leaders

- The headteacher is responsible for ensuring the e-safety of members of the school community and will manage the education of pupils and training of staff in e-safety and awareness of potential radicalisation in pupils.

- The headteacher will take appropriate action if it is felt that any pupil of the school may be becoming radicalised.

- The headteacher, together with the data protection officer, is responsible on a day-to-day basis for ensuring compliance with the Data Protection Act and GDPR for the processing of personal data.

- The headteacher and another member of the senior leadership team/e-safety co-ordinator will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff, including the headteacher.

- The Education and Inspections Act 2006 empowers the headteacher, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, even though they may take place out of school, but are linked to membership of the school.

Roles and responsibilities – e-safety co-ordinator

The e-safety co-ordinator: David White – Deputy Headteacher & Safeguarding Lead, e-safety co-ordinator.

- Leads the e-safety committee to support policy & systems review

- Takes day-to-day responsibility for e-safety issues working with Key Stage Leader DSLs and has a leading role in establishing and reviewing the school e-safety policy and other related policies, including working with the GDPR Manager to ensure the safe processing of personal data.

- Ensures that all members of staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

- Provides training and advice for staff in liaison with the PSHCE lead to ensure that all teaching is carried out in an age-appropriate way.

- Liaises with school ICT technical staff.

- Reports regularly to the senior leadership team/headteacher.

- Will receive training at regular update sessions and by reviewing national and local guidance documents.

- Liaises with the local authority (LA) and reports to the headteacher any suspicions of pupils who may be becoming radicalised.

Roles and responsibilities – network manager/technical support provider

The network managers (Arpit Bhargava) or technical support provider is responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.

- That appropriate filters and monitoring systems are in place.

- That the school meets the e-safety technical requirements outlined in the relevant national/local ICT security policy and/or acceptable usage/e-safety policy and guidance.

- Users may only access the school's networks through a properly enforced password protection policy.

- The headteacher is informed of any breaches in the processing of personal data.

- The network manager/technical support provider will receive appropriate training on a regular basis from approved trainers to support the e-safety of all members of the school community.

- The relevant DSLs and headteacher is informed of any suspicions of pupils who may be becoming radicalised.

Roles and responsibilities – teaching and support staff
All staff receive e-safety training as part of annual safeguarding training and understand their responsibilities, as outlined in this policy. An audit of the e-safety training needs of all staff will be carried out regularly. Training will be offered as a planned programme of formal e-safety training available to all staff. All new staff will receive e-safety training as part of their safeguarding induction programme, ensuring that they fully understand the school e-safety policy and acceptable usage policies.

The school uses annual safeguarding training and Educare (training modules) to ensure that staff are trained and familiar with eSafety risks and policy requirements.

Teaching and support colleagues are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current school e-safety policy.

- They have read, understood and signed the relevant staff acceptable computer usage. agreement and staff laptop usage agreement, as well as other related policies e.g. staff e-mail, social media, use of personally owned ICT devices and professional identity protection.

- They report any suspected misuse or problem to the relevant DSL using SIMs behaviour, this must also be logged on MyConcern if a safeguarding concern. Year Leaders & Key Stage Leaders will be informed to support investigation of reported incidents and to support students involved. Sanctions will be issued in line with school behaviour policy.

- They report any suspected breach of processing any personal data to the DSL and or Headteacher and if a safeguarding concern must also be logged on MyConcern. Investigation will be initiated by the Year Leader/Key Stage Leader and or e-safety co-ordinator as appropriate for investigation.

- Digital communications with pupils (email/virtual learning environment (VLE)/voice) are on a professional level and only carried out using official school systems.

- Pupils understand and follow the school e-safety policy and the pupil acceptable computer usage policy.

- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- They monitor ICT activity in lessons and in extracurricular and extended school activities.

- They are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.

- They are aware of the e-safety issues pertaining to email and social media usage.

- They are alert to, and report to the headteacher, any suspicions of pupils who may be becoming radicalised.

- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Roles and responsibilities – designated safeguarding lead/designated person for child protection/child protection officer
The designated safeguarding lead and supporting DSLs are trained in e-safety issues and will be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.

- Access to illegal/inappropriate materials.

- Inappropriate online contact with adults/strangers.

- Potential or actual incidents of grooming.

- Cyber-bullying.

- Sexting.

- Suspicions of radicalisation.

Roles and responsibilities – e-safety group
Members of the e-safety group:

Link governor (Matthew Williams) e-safety co-ordinator (David White) staff members – PSHCE lead & line manager (Alicia Crix), Network manager, (Arpit Bhargava), student member, parent representative or parent governor) and will assist with the development of e-safety education.

Roles and responsibilities – pupils

The rules for safe use of ICT systems/internet will be posted in all relevant rooms and displayed on log-on screens so that pupils are aware of their responsibilities.

Pupils:

- Are responsible for using the school ICT systems in accordance with the pupil acceptable computer usage policy and agreement, which they will be expected to understand and sign this agreement with their parents before being given access to school systems.

- Visiting pupils, e.g. from local feeder schools, will be expected to understand and sign the visiting pupil acceptable computer usage agreement before access is authorised.

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials, including suspicions of pupils who may be becoming radicalised, and know how to report such abuse.

- Will develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices, including the school's policy on confiscation of inappropriate items where it relates to the use of mobile phones.

- Will be expected to know and understand school policies on the taking/use of images and on cyber-bullying.

- Will be expected to know and understand the dangers of social networking sites as well as their benefits.

- Will understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school.

Roles and responsibilities – parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

Parents and carers will be responsible for endorsing (by signature) the pupil acceptable computer usage agreement as part of the school's induction process.

Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through:

- Sharing information on internet safety (online safety section of the school website) and the importance of monitoring internet use at home to all parents annually – using the school's online safety area on the school website

- Parents' Year Ahead events and student transition and induction events

- Newsletters – latest information on e-Safety

- Information about all relevant national/local e-safety campaigns/literature.

- Information about useful organisations /support services for reporting e-safety issues (see appendix 2 and the school's website links).

E-safety in the curriculum

E-safety is taught in specific areas of the curriculum but is also emphasised whenever pupils are using computers online. Elthorne Park High school has a weekly PSHCE lesson that integrates eSafety themes across all year groups. This curriculum provision is reviewed annually to keep up with ever changing IT risks.

Staff always consider age-appropriateness when speaking of e-safety and will be aware of those pupils who may be particularly vulnerable, e.g. looked-after children or those with special needs. The school may use external resources and external visitors to assist in lessons, but appropriate members of staff will check in advance to ensure that they will enhance lessons and that materials used are appropriate for them.

In PSHCE lessons and as part of SRE curriculum delivery:

Pupils are taught about:

- Online safety and harm.
- Positive, healthy and respectful relationships online.
- The effects of their online actions.
- How to recognise and show respectful behaviour online.

Computing in the curriculum
- Principles of online safety.
- Where to obtain help and support if they are concerned about any online content or contact.

Citizenship in the curriculum
- Media literacy online.
- Distinguishing fact from fiction online.

E-safety throughout the curriculum
Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities, including:

- How to evaluate what they see online – to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- How to recognise persuasion techniques.
- How to recognise acceptable and unacceptable online behaviour – to understand the need for the acceptable computer usage agreement and to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- How to identify online risks.
- How and when to seek support.
- The need to acknowledge the source of any information used and to respect copyright when using material accessed on the internet.

In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.

Where pupils are allowed to search the internet freely, e.g. using search engines, staff are vigilant in monitoring the content of the websites the pupils visit.

It is accepted that from time-to-time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the network manager temporarily removes those sites from the filtered list for the period of study. Any request to do so will be recorded, with clear reasons for the need.

Management of infrastructure
The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the acceptable computer usage policy and any relevant LA e-safety policy and guidance.

- Personal data is held and processed in compliance with the Data Protection Act and GDPR. Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. See Elthorne Park High school's GDPR and e-mail policy.

- There will be regular reviews (weekly student filter report) and audits of the safety and security of school ICT systems.

- Servers, wireless systems and cabling will be securely located and physical access restricted.

- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the network manager and will be reviewed, at least annually in consultation with the Headteacher.

- All users will be provided with a username and password by the network manager.

- The 'master/administrator' passwords for the school ICT system, used by the network manager (or other person) are also available to the Headteacher.

- Users are made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- The school maintains and supports the managed monitoring and filtering service provided by London Grid for Learning, Smoothwall and Impero.

- Any filtering issues should be reported immediately to the network manager.

- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the acceptable computer usage policy.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

- An agreed policy is in place in the acceptable computer usage policy regarding the downloading of executable files by users.

- Agreements are signed by members of staff in possession of school-provided laptops/devices regarding the extent of personal use that users (staff/pupils/community users) and their family members are permitted.

- The school infrastructure and individual workstations are protected by up-to-date virus software.

- The IT network lead is responsible for producing a weekly report of student use/searches any safeguarding concerns are brought the attention of Key Stage DSLs for further investigation and support.

Protocols on using digital and video images

- When using digital images, staff inform and educate pupils about the risks associated with taking, using, sharing, publishing and distributing images. In particular, they recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- If any incidents come to light about ‘sexting’ i.e. the sharing of sexual images of pupils under 18, the designated safeguarding lead should be advised in the first instance.

- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.

- Any images should only be taken on school equipment. Personal equipment of staff should *not* be used for such purposes.

- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Written permission from parents or carers will be obtained. Permissions are obtained as part of the school’s admissions process and recorded on the school’s management database.

Protocols on data protection
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act and in compliance with the General Data Protection Regulation which state that personal data must be:

- Fairly and lawfully processed.

- Processed for limited purposes.

- Adequate, relevant and not excessive.

- Accurate.

- Kept no longer than is necessary.

- Processed in accordance with the data subject’s rights.

- Secure.

- Only transferred to others with adequate protection.

Staff will ensure that they comply with the internal data security policy by:

- Taking care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Using personal data only on secure password protected computers and other devices, and ensuring that they are properly ‘logged-off’ at the end of any session in which they are using personal data.

- Transferring data using encryption and secure password protected devices.

Protocols for handling electronic communications
When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.

- Users need to be aware that email communications may be monitored.

- Users will be expected to know and understand school policies on email, social media (and other relevant electronic devices protocols.)

- Users must immediately report, to the nominated person (Designated Safeguarding lead of Headteacher), in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Users must not respond to any such email but must follow the procedures in the email policy.

- Any digital communication between staff and pupils or parents/carers (email, chat, VLE etc) must be professional in tone and content.

Unsuitable/inappropriate activities
Certain activities are referred to in the acceptable computer usage agreements as being inappropriate in a school context and users must not engage in these activities in school or outside school when using school equipment or systems. The school policies on child protection, safeguarding and e-safety *must be* followed if any apparent, suspected or actual misuse appears to involve illegal or inappropriate activity e.g.:

- Child sexual abuse images.

- Adult material which potentially breaches the Obscene Publications Act.

- Criminally racist material.

- Other criminal conduct, activity or materials.

- Potential radicalisation of pupils.

Should any serious e-safety incidents take place, the appropriate external authorities will be informed e.g. local area designated safeguarding lead, police etc or, for personal data breaches, the Information Commissioner's Office (ICO).

Monitoring and reviewing

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity (i.e. ISP, school network or managed service as appropriate).
- Internal monitoring data for network activity.
- Surveys/questionnaires of pupils, parents/carers and staff as part of the school's QA procedures and PSHCE curriculum review.

The policy will be reviewed by the governors biennially, or more regularly, in the light of any new legislation, any incidents that have taken place, significant new developments in the use of the technologies, or perceived new threats to e-safety as advised by the e-safety committee or others.

Next review due: March 2024

APPENDIX 1

Acts of Parliament relevant to e-safety in schools

Communications Act 2003 (section 127)
Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is an offence liable, on conviction, to imprisonment. (This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.)

Computer Misuse Act 1990 (sections 1–3)
Regardless of an individual's motivation, the Act makes it a criminal offence to:

- Gain access to computer files or software without permission (eg using someone else's password to access files).
- Gain unauthorised access, as above, in order to commit a further criminal act (such as fraud).
- Impair the operation of a computer or program (eg caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Copyright, Designs and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her 'work' without permission.

The material to which copyright may attach (known in the business as 'work') must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Counter-Terrorism and Security Act 2015 (section 26)
The prevent duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities, in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 empowers courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Criminal Justice and Immigration Act 2008 (section 63)
It is an offence to possess an 'extreme pornographic image'. An extreme pornographic image is defined in section 63 of this Act. Penalties can be up to three years imprisonment.

Data Protection Act 1998
The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and data users must comply with important data protection principles when handling personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

Education and Inspections Act 2006
Education and Inspections Act 2006 outlines legal powers for schools which relate to cyber-bullying/bullying:

- Headteachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils off-site.

- School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy.

General Data Protection Regulation (GDPR)
The General Data Protection Regulation became effective in May 2018 and is legislation designed to strengthen and unify the safety and security of all data held by organisations within the European Union. In EU legislative terms, it updates and replaces the 1995 Directive. In national UK terms, it replaces the current 1998 Data Protection Act.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message that conveys indecent, grossly offensive, threatening material or information that is false, or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This can include racist, xenophobic and homophobic comments, messages etc.

Obscene Publications Act 1959 and 1964
Publishing an 'obscene' article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows, or ought to know, that his course of conduct will cause the other so to fear on each of those occasions.

This also includes incidents of racism, xenophobia and homophobia.

Public Order Act 1986 (sections 17–29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006, it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Regulation of Investigatory Powers Act 2000
The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

However, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 permit a degree of monitoring and record keeping, (eg to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network.) Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Sexual Offences Act 2003
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the UK. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as ‘sexting’). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust. Any sexual intercourse with a child under the age of 13 commits the offence of rape.

APPENDIX 2

Useful organisations/support services for reporting e-safety issues

Grooming or other illegal behaviour
If you want to report someone who is behaving suspiciously online towards a child, you should in an emergency contact the emergency services by calling 999, or otherwise make a report to *Child Exploitation Online Protection Centre (CEOP)*. See www.ceop.gov.uk.

Criminal content online
If you stumble across criminal content online, you should report this to the *Internet Watch Foundation (IWF)* at https://iwf.org.uk

Criminal content in the UK includes child sexual abuse images, criminally obscene adult content as well as non-photographic child sexual abuse images.

Online content which incites hatred on the grounds of race, religion and sexual orientation should be reported to *True Vision*, which tackles all forms of hate crime, including those on the grounds of disability and transgender identity. True Vision, at www.report-it.org.uk, will give you information on content which incites hatred and how to report it.

Getting help/advice: for young people
- ChildLine: Is a free 24/7 helpline for children and young people. Visit www.childline.org.uk or call 0800 1111. ChildLine is run by the NSPCC.

Getting help/advice: for parents
- *Family Lives*: A charity providing help and support in all aspects of family life. They have a 24/7 free Parentline on 0808 8002222, or visit www.familylives.org.uk

- *Kidscape*: Is a leading anti-bullying charity, which provides a helpline for parents of children who have been bullied. From 10am to 5pm, Mondays and Tuesdays on 0207 823 5430 www.kidscape.org.uk.

- *Childnet International* Is a non-profit organisation working to help make the internet a safe place for children. 'We strive to take a balanced approach, making sure that we promote the positive opportunities, as well as responding to the risks and equipping children and young people to deal with them'. Contact details are: www.childnet.com phone 020 7639 6967, email info@childnet.com.

- *UK council for internet safety (UKCIS)* has practical guides to help parents and others with internet safety www.gov.uk/government/organisations/uk-council-for-internet-safety.

- *Thinkuknow* has a section for parents which offers advice on protecting children from abuse online offered by the National Crime Agency's CEOP Command www.thinkuknow.co.uk/parents.

Getting help/advice: for teachers
DFE has a telephone helpline (0207 340 7264) and an email address (counter.extremism@education.gov.uk) to enable teachers to raise concerns or questions on extremism directly with them.